

SENATE/HOUSE FILE \_\_\_\_\_  
BY (PROPOSED ATTORNEY GENERAL  
BILL)

**A BILL FOR**

1 An Act modifying certain provisions relating to personal  
2 information security breach protection.  
3 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

1 Section 1. Section 715C.1, subsections 1, 5, and 11, Code  
2 2018, are amended to read as follows:

3 1. "*Breach of security*" means unauthorized acquisition,  
4 or reasonable belief of unauthorized acquisition, of personal  
5 information maintained in computerized any form, including  
6 but not limited to electronic or paper form, by a person that  
7 compromises the security, confidentiality, or integrity of  
8 the personal information. "*Breach of security*" also means  
9 unauthorized acquisition of personal information maintained  
10 by a person in any medium, including on paper, that was  
11 transferred by the person to that medium from computerized  
12 form and that compromises the security, confidentiality, or  
13 integrity of the personal information. Good faith acquisition  
14 of personal information by a person or that person's employee  
15 or agent for a legitimate purpose of that person is not a  
16 breach of security, provided that the personal information  
17 is not used in violation of applicable law or in a manner  
18 that harms or poses an actual threat to the security,  
19 confidentiality, or integrity of the personal information.

20 5. "*Encryption*" means the use of an one-hundred-twenty-  
21 eight-bit or higher algorithmic process to transform data into  
22 a form in which the data is rendered unreadable or unusable  
23 without the use of a confidential process or key.

24 11. a. "*Personal information*" means an individual's first  
25 name or first initial and last name in combination with any  
26 one or more of the following data elements that relate to the  
27 individual if any of the data elements are not encrypted,  
28 redacted, or otherwise altered by any method or technology in  
29 such a manner that the name or data elements are unreadable or  
30 are encrypted, redacted, or otherwise altered by any method or  
31 technology but the keys to unencrypt, unredact, or otherwise  
32 read the data elements have been obtained through the breach  
33 of security:

34 (1) Social security number.

35 (2) Driver's license number or other unique identification

1 number created or collected by a government body.

2 (3) Financial account number, credit card number, or debit  
3 card number ~~in combination with any required expiration date,~~  
4 ~~security code, access code, or password that would permit~~  
5 ~~access to an individual's financial account.~~

6 (4) Unique electronic identifier or routing code, in  
7 combination with any required security code, access code, or  
8 password that would permit access to an individual's financial  
9 account.

10 (5) Unique biometric data, such as a fingerprint, retina or  
11 iris image, or other unique physical representation or digital  
12 representation of biometric data.

13 (6) Medical information, including but not limited to  
14 information regarding an individual's medical history, mental  
15 or physical condition, or medical treatment or diagnosis by a  
16 health care professional.

17 (7) Health insurance information, including but not limited  
18 to an individual's health insurance policy number, subscriber  
19 identification number, or any unique identifier used by a  
20 health insurer to identify an individual.

21 (8) Tax identification number.

22 b. "Personal information" also includes a financial account  
23 number, credit card number, or debit card number alone.

24 c. "Personal information" also includes an account username  
25 or electronic mail address, in combination with any required  
26 password or account security information that would permit  
27 access to an individual's online account.

28 b. d. "Personal information" does not include information  
29 that is lawfully obtained from publicly available sources, or  
30 from federal, state, or local government records lawfully made  
31 available to the general public.

32 Sec. 2. Section 715C.2, subsections 1, 6, 7, and 8, Code  
33 2018, are amended to read as follows:

34 1. Any person who owns or licenses ~~computerized~~ data that  
35 includes a consumer's personal information that is used in

1 the course of the person's business, vocation, occupation,  
2 or volunteer activities and that was subject to a breach  
3 of security shall give notice of the breach of security  
4 following discovery of such breach of security, or receipt  
5 of notification under subsection 2, to any consumer whose  
6 personal information was included in the information that was  
7 breached. The consumer notification shall be made in the most  
8 expeditious manner possible and without unreasonable delay,  
9 but no later than forty-five days after the discovery of such  
10 breach of security or receipt of notification under subsection  
11 2, consistent with the legitimate needs of law enforcement as  
12 provided in subsection 3, and consistent with any measures  
13 necessary to sufficiently determine contact information for  
14 the affected consumers, determine the scope of the breach, and  
15 restore the reasonable integrity, security, and confidentiality  
16 of the data.

17 6. a. Notwithstanding subsection 1, notification is not  
18 required if, after an appropriate investigation or after  
19 consultation with the relevant federal, state, or local  
20 agencies responsible for law enforcement, the person determined  
21 that no reasonable likelihood of ~~financial~~ harm to the  
22 consumers whose personal information has been acquired has  
23 resulted or will result from the breach. Such a determination  
24 must be documented in writing and the documentation must be  
25 maintained for five years.

26 b. In the event that notification is not required pursuant  
27 to this subsection, the person shall provide the written  
28 determination required in paragraph "a" to the director of the  
29 consumer protection division of the office of the attorney  
30 general within five business days after documenting such  
31 determination.

32 7. ~~This section does~~ Subsections 1 through 6 shall not apply  
33 to any of the following:

34 a. A person who complies with notification requirements or  
35 breach of security procedures that provide greater protection

1 to personal information and at least as thorough disclosure  
2 requirements than that provided by this section pursuant to  
3 the rules, regulations, procedures, guidance, or guidelines  
4 established by the person's primary or functional federal  
5 regulator.

6     *b.* A person who complies with a state or federal law  
7 that provides greater protection to personal information and  
8 at least as thorough disclosure requirements for breach of  
9 security or personal information than that provided by this  
10 section.

11     *c.* A person who is subject to and complies with regulations  
12 promulgated pursuant to Tit. V of the Gramm-Leach-Bliley Act of  
13 1999, 15 U.S.C. §6801 – 6809.

14     8. Any person who owns or licenses ~~computerized~~ data  
15 that includes a consumer's personal information that is  
16 used in the course of the person's business, vocation,  
17 occupation, or volunteer activities and that was subject to a  
18 breach of security requiring notification to more than five  
19 ~~hundred residents of this state~~ consumers pursuant to ~~this~~  
20 ~~section subsection 1~~ or any of the laws, rules, regulations,  
21 procedures, guidance, or guidelines set forth in subsection  
22 7 shall give written notice of the breach of security  
23 ~~following discovery of such breach of security, or receipt~~  
24 ~~of notification under subsection 2,~~ to the director of the  
25 consumer protection division of the office of the attorney  
26 general within five business days after giving notice of the  
27 breach of security to any consumer pursuant to this section.  
28 The written notice shall include the following:

29     *a.* A sample copy of any notification sent to consumers.

30     *b.* The approximate number of consumers affected or  
31 potentially affected by the breach of security.

32     *c.* A description of any services offered to consumers  
33 affected or potentially affected by the breach of security, and  
34 instructions as to how consumers may use such services.

35     *d.* The name, address, telephone number, and electronic mail

1 address of an individual who may be contacted by the consumer  
2 protection division of the office of the attorney general for  
3 any additional information about the breach of security.

4 e. The federal employer identification number of the  
5 person, which the consumer protection division of the office of  
6 the attorney general may share with any state agency for the  
7 purpose of fraud detection. Notwithstanding chapter 22 or any  
8 other provision of law to the contrary, the federal employer  
9 identification number shall be maintained in a separate  
10 confidential file or other confidential medium.

11 EXPLANATION

12 The inclusion of this explanation does not constitute agreement with  
13 the explanation's substance by the members of the general assembly.

14 This bill modifies various provisions relating to personal  
15 information security breach protection.

16 The bill makes several changes to the definitions listed  
17 in Code section 715C.1. The bill expands the definition of  
18 "breach of security" to include the reasonable belief of  
19 unauthorized acquisition of personal information, which may  
20 be in any form, including electronic or paper form. However,  
21 the bill removes the unauthorized acquisition of personal  
22 information that was transferred from computerized form to  
23 another medium from the definition of "breach of security".  
24 The definition of "encryption" is modified to mean the use of  
25 an 128-bit or higher algorithmic process. The bill modifies  
26 the definition of "personal information" by providing that  
27 it may include a financial account number, credit card  
28 number, or debit card number alone. The bill also includes  
29 certain medical information, health insurance information,  
30 tax information, and electronic account information in the  
31 definition of "personal information".

32 Current law requires a person who owns or licenses personal  
33 information that is subject to a breach of security to give  
34 notice to affected consumers in the most expeditious manner  
35 possible and without unreasonable delay. The bill provides

1 that such notice to affected consumers must occur no later than  
2 45 days after the discovery of the breach of security.

3 Current law provides that a person who owns or licenses  
4 personal information that is subject to breach of security does  
5 not need to provide notification of the security breach to  
6 affected consumers if the person makes a written determination  
7 that there is no reasonable likelihood of financial harm to  
8 affected consumers. The bill removes the term "financial",  
9 allowing a person to refrain from providing notification if  
10 the person makes a written determination that there is no  
11 reasonable likelihood of harm to affected consumers. The  
12 bill also requires a person who makes such a determination  
13 to provide this written determination to the director of the  
14 consumer protection division of the office of the attorney  
15 general within five business days after documenting the  
16 determination.

17 Current law requires a person who owns or licenses personal  
18 information that is subject to a breach of security requiring  
19 notification to more than 500 consumers in the state, as  
20 required by Code section 715C.2, to give written notice  
21 of the breach of security to the director of the consumer  
22 protection division of the office of the attorney general.  
23 The bill provides that written notification to the attorney  
24 general is also required for breaches of security where  
25 written notification to more than 500 consumers in the state  
26 is required by a person's primary or functional federal  
27 regulator, a state or federal law that gives greater protection  
28 to personal information than provided in Code section 715C.2,  
29 or certain federal law. The bill also specifies that written  
30 notification to the attorney general must include a sample  
31 copy of any notification sent to consumers, the approximate  
32 number of affected or potentially affected consumers, a  
33 description of any services offered to affected consumers,  
34 contact information for an individual who may be contacted  
35 for additional information regarding the breach of security,

S.F. \_\_\_\_\_ H.F. \_\_\_\_\_

1 and a federal employer identification number, which will be  
2 maintained in a confidential file.